

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-091456

(43)Date of publication of application : 27.03.2002

(51)Int.Cl.

G10K 15/02
G09C 1/00
G10L 19/00
H04B 7/26
H04L 9/08
H04L 9/32
H04M 1/00
H04M 1/02
H04M 1/725
H04M 11/00

(21)Application number : 2000-285058

(71)Applicant : SANYO ELECTRIC CO LTD

(22)Date of filing : 20.09.2000

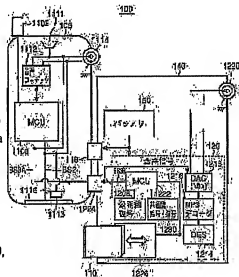
(72)Inventor : HORI YOSHIHIRO
OTA SEIYA

(54) PORTABLE TELEPHONE SET AND ADAPTER TO BE USED FOR THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a portable telephone set capable of receiving, decoding, and reproducing enciphered music data without largely changing the constitution of a conventional portable telephone set, and an adapter to be used for the portable telephone set.

SOLUTION: A portable telephone set 100 is constituted of a main body 105 and an adapter 140. The adapter 140 is provided with a data terminal 120, a battery 150, and a jack 1220. The data terminal equipment 120 records the enciphered music data received by the main body 105 in a memory card 110 mounted on an attaching/detaching part 1226. Also, the data terminal equipment 120 reads and decodes the enciphered music data from the memory card 110 by using a public key decoding part 1206, a common key enciphering and decoding part 1230, and a DES 1214. Then, the data terminal equipment 120 defrosts and reproduces the music data by an MP3 decoder 1216, and outputs the music data to a jack 1220.



(51) Int.Cl. ⁷	識別記号	F I	テマコード ⁸ (参考)
G 1 0 K 15/02		G 1 0 K 15/02	5 J 1 0 4
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 Z 5 K 0 2 3
G 1 0 L 19/00		H 0 4 M 1/00	R 5 K 0 2 7
H 0 4 B 7/26		1/02	C 5 K 0 6 7
H 0 4 L 9/08		1/725	5 K 1 0 1

審査請求 未請求 請求項の数19 O L (全 28 頁) 最終頁に続く

(21) 出願番号 特願2000-285058(P2000-285058)

(22) 出願日 平成12年9月20日 (2000.9.20)

(71) 出願人 00001889

三洋電機株式会社

大阪府守口市京阪本通 2 丁目 5 番 5 号

(72) 発明者 堀 吉宏

大阪府守口市京阪本通 2 丁目 5 番 5 号 三
洋電機株式会社内

(72) 発明者 太田 晴也

大阪府守口市京阪本通 2 丁目 5 番 5 号 三
洋電機株式会社内

(74) 代理人 100064746

弁理士 深見 久郎 (外 3 名)

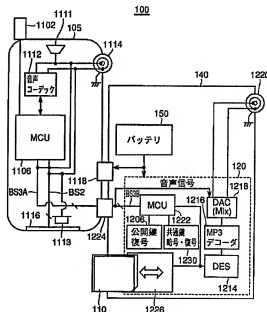
最終頁に続く

(54) 【発明の名称】 携帯電話機およびそれに用いるアダプタ

(57) 【要約】

【課題】 従来の携帯電話機の構成を大幅に変更することなく、暗号化音楽データの受信、復号および再生を行なうことができる携帯電話機およびそれに用いるアダプタを提供する。

【解決手段】 携帯電話機 100 は、本体 105 とアダプタ 140 とから成る。アダプタ 140 は、データ端末装置 120 と、バッテリー 150 と、ジャック 1220 とを含む。データ端末装置 120 は、本体 105 によって受信された暗号化音楽データ等を着脱部 1228 に装着されたメモリカード 110 へ記録する。また、データ端末装置 120 は、公開鍵復号部 1206、共通鍵暗号・復号部 1230、および DES 1214 によってメモリカード 110 から暗号化音楽データを読出し、および復号を行なう。そして、データ端末装置 120 は、MP3 デコーダ 1218 によって音楽データを解凍して再生し、ジャック 1220 へ出力する。



【特許請求の範囲】

【請求項1】 音楽データを暗号化した暗号化音楽データと、前記暗号化音楽データを復号して前記音楽データを復元するための復号鍵であるライセンス鍵とを記録したデータ記録装置から前記暗号化音楽データと前記ライセンス鍵とを取得して前記音楽データを再生する携帯電話機であって、

本体部と、
前記本体部から脱着可能なアダプタとを備え、
前記アダプタは、
前記データ記録装置を脱着する着脱部と、
データ端末装置とを含み、
前記データ端末装置は、
前記データ記録装置とデータの授受を行なうためのインタフェース部と、
前記ライセンス鍵によって前記暗号化音楽データを復号して前記音楽データを復元する復号処理部と、
前記復号処理部にて復元された音楽データから音楽を再生する音楽再生部と、制御部とを含み、
音楽データの再生時、

前記制御部は、前記データ記録装置に記録された前記暗号化音楽データおよび前記ライセンス鍵を前記インタフェース部を介して取得し、その取得した暗号化音楽データおよびライセンス鍵を前記復号処理部に与える、携帯電話機。

【請求項2】 音楽データを暗号化した暗号化音楽データおよび/または前記暗号化音楽データを復号して前記音楽データを復元するための復号鍵であるライセンス鍵を受信してデータ記録装置に記録する携帯電話機であって、

本体部と、
アダプタとを備え、
前記アダプタは、
前記データ記録装置を脱着する着脱部と、
データ端末装置とを含み、
前記データ端末装置は、
前記データ記録装置とデータの授受を行なうためのインタフェース部と、
制御部とを含み、
データの受信時、
前記制御部は、前記本体部から前記暗号化音楽データおよび/または前記ライセンス鍵を受取り、その受取った暗号化音楽データおよび/またはライセンス鍵を前記インタフェース部を介して前記データ記録装置に記録する、携帯電話機。

【請求項3】 音楽データを暗号化した暗号化音楽データおよび/または前記暗号化音楽データを復号して前記音楽データを復元するための復号鍵であるライセンス鍵をデータ記録装置に記録し、または前記データ記録装置に記録された前記暗号化音楽データと前記ライセンス鍵

とを取得して前記音楽データを再生する携帯電話機であって、
本体部と、

アダプタ部とを備え、
前記アダプタ部は、
前記データ記録装置を脱着する着脱部と、
データ端末装置とを含み、
前記データ端末装置は、

前記データ記録装置とデータの授受を行なうためのインタフェース部と、
前記データ記録装置に対する認証データを保持する認証データ保持部と、
前記ライセンス鍵によって前記暗号化音楽データを復号する復号処理部と、
制御部とを含み、
データの受信時、

前記制御部は、前記本体部から前記暗号化音楽データおよび/または前記ライセンス鍵を受取り、その受取った暗号化音楽データおよび/またはライセンス鍵を前記インタフェース部を介して前記データ記録装置に記録し、
データの再生時、

前記制御部は、前記認証データを前記インタフェース部を介して前記データ記録装置へ送り、前記データ記録装置において前記認証データが認証されることによって前記データ記録装置から送られて来るライセンス鍵および暗号化音楽データを前記復号処理部へ入力する、携帯電話機。

【請求項4】 前記アダプタ部は、前記データ端末装置から出力される音楽データの再生信号を外出力装置へ出力するための音楽端子をさらに含む、請求項1または請求項3に記載の携帯電話機。

【請求項5】 前記本体部は、通話時に相手側から受取った音声信号を外部へ出力し、音声信号を入力するための音声端子を含む、請求項4に記載の携帯電話機。

【請求項6】 前記音楽端子は、2チャンネルの出力信号を前記外部へ出力する、請求項4または請求項5に記載の携帯電話機。

【請求項7】 前記本体部は、前記データ端末装置から出力される音楽データの再生信号と、通話時に相手側から受取った音声信号とを外出力装置へ出力し、音声信号を入力するための音楽音声端子を含む、請求項1または請求項3に記載の携帯電話機。

【請求項8】 前記音楽音声端子は、2チャンネルの出力信号を前記外部出力装置へ出力する、請求項7に記載の携帯電話機。

【請求項9】 前記データ端末装置は、前記データ記録装置から前記ライセンス鍵を取得するための第1のセッション鍵を発生するセッション鍵発生部と、

前記バスに接続され、前記データ記録装置における前記

認証データの認証に基づいて、前記データ記録装置から取得した第2のセッション鍵によって前記第1のセッション鍵を暗号化する暗号処理部とをさらに含み、前記復号処理部は、

前記パスに接続され、前記第1のセッション鍵によって暗号化された前記ライセンス鍵を復号する第1の復号処理部と、

前記パスに接続され、前記第1の復号処理部において復号された前記ライセンス鍵によって前記暗号化音楽データを復号する第2の復号処理部とから成り、データの再生時、

前記制御部は、さらに、前記第2のセッション鍵を前記暗号処理部へ与え、前記第1のセッション鍵によって暗号化されたライセンス鍵を前記第1の復号処理部へ与え、前記暗号化音楽データを前記第2の復号処理部へ与える、請求項1から請求項8のいずれか1項に記載の携帯電話機。

【請求項10】 前記データ端末装置は、前記パスに接続され、前記認証データに含まれる公開暗号鍵と非対称な秘密復号鍵を保持する鍵保持部と、前記パスに接続され、前記公開暗号鍵によって暗号化された前記第2のセッション鍵を前記秘密復号鍵によって復号する第3の復号処理部とをさらに含み、データの再生時、

前記制御部は、さらに、前記公開暗号鍵によって暗号化された前記第2のセッション鍵を前記データ記録装置から受取り、前記第3の復号処理部へ与え、前記第3の復号処理部において復号された第2のセッション鍵を前記暗号処理部へ与える、請求項9に記載の携帯電話機。

【請求項11】 前記本体部は、前記データ端末装置を駆動する駆動電源を含む、請求項1から請求項10のいずれか1項に記載の携帯電話機。

【請求項12】 前記アダプタ部は、前記データ端末装置を駆動する駆動電源をさらに含み、請求項1から請求項10のいずれか1項に記載の携帯電話機。

【請求項13】 音楽データを暗号化した暗号化音楽データと、前記暗号化音楽データを復号して前記音楽データを復元するための復号鍵であるライセンス鍵とを記録したデータ記録装置から前記暗号化音楽データと前記ライセンス鍵とを取得して前記音楽データを再生する携帯電話機に装着するアダプタであって、前記データ記録装置を脱着する着脱部と、データ端末装置とを備え、前記データ記録装置は、前記データ記録装置とデータの授受を行なうためのインタフェース部と、前記データ記録装置に対する認証データを保持する認証データ保持部と、前記ライセンス鍵によって前記暗号化音楽データを復号する復号処理部と、

制御部とを含み、

音楽データの再生時、

前記制御部は、前記認証データを前記インタフェース部を介して前記データ記録装置へ送り、前記データ記録装置において前記認証データが認証されることによって前記データ記録装置から送られてくる前記ライセンス鍵および前記暗号化音楽データを受取り、その受取った暗号化音楽データおよびライセンス鍵を前記復号処理部に与える、アダプタ。

- 10 【請求項14】 音楽データを暗号化した暗号化音楽データおよび/または前記暗号化音楽データを復号して前記音楽データを復元するための復号鍵であるライセンス鍵を受信してデータ記録装置に記録する携帯電話機に装着するアダプタであって、前記データ記録装置を脱着する着脱部と、データ端末装置とを備え、前記データ端末装置は、

前記データ記録装置とデータの授受を行なうためのインタフェース部と、

- 20 制御部とを含み、

データの受信時、

前記制御部は、前記携帯電話機から前記暗号化音楽データおよび/または前記ライセンス鍵を受取り、その受取った暗号化音楽データおよび/またはライセンス鍵を前記インタフェース部を介して前記データ記録装置に記録する、アダプタ。

- 【請求項15】 音楽データを暗号化した暗号化音楽データおよび/または前記暗号化音楽データを復号して前記音楽データを復元するための復号鍵であるライセンス鍵とを受信してデータ記録装置に記録し、または前記データ記録装置に記録された前記暗号化音楽データと前記ライセンス鍵とを取得して前記データを再生する携帯電話機に装着するアダプタであって、

前記データ記録装置を脱着するための着脱部と、データ端末装置とを備え、前記データ端末装置は、前記データ記録装置とデータの授受を行なうためのインタフェース部と、

前記データ記録装置に対する認証データを保持する認証データ保持部と、

- 40 前記ライセンス鍵によって前記暗号化音楽データを復号する復号処理部と、

制御部とを含み、

データの受信時、

前記制御部は、前記携帯電話機から前記暗号化音楽データおよび/または前記ライセンス鍵を受取り、その受取った暗号化音楽データおよび/またはライセンス鍵を前記インタフェース部を介して前記データ記録装置に記録し、

- 50 データの再生時、

前記制御部は、前記認証データの前記インタフェース部を介して前記データ記録装置へ送り、前記データ記録装置において前記認証データが認証されることによって前記データ記録装置から送られてくる前記ライセンスおよび前記暗号化音楽データを受取り、その受取ったライセンス鍵および暗号化音楽データを前記復号処理部へ入力する。アダプタ。

【請求項16】 前記データ端末装置から出力される音楽データの再生信号を外部出力装置へ出力するための音楽端子をさらに含む、請求項13または請求項15に記載のアダプタ。

【請求項17】 前記データ端末装置の駆動電源をさらに備える、請求項11から請求項16のいずれか1項に記載のアダプタ。

【請求項18】 前記携帯電話機に対して駆動電源を供給する、請求項17に記載のアダプタ。

【請求項19】 前記携帯電話機から駆動電源の供給を受ける、請求項13から請求項16のいずれか1項に記載のアダプタ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられる携帯電話機およびそれに用いられるアダプタに関するものである。

【0002】

【従来の技術】 近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】 このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】 したがって、このような情報通信網において音楽データや画像データ等の著作権者の権利が存在する創作物が伝送される場合、適切な著作権保護のための方法が取られないと、著しく著作権者の権利が侵害され、著しくおそれがある。

【0005】 一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利となる。

【0006】 ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）につい

ては、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金うちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】 しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】 このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自身が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な策が講じられる必要がある。

【0009】 この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】 そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書で暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】 最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリに記録する。

【0012】

【発明が解決しようとする課題】 しかし、暗号化音楽コンテンツデータを配信サーバから受信し、その受信した暗号化音楽データを記録したり、復号および再生するためには、従来の携帯電話機における通常の電話機能の他

にメモリカードを制御し、メモリカードからの暗号化音楽コンテンツデータを復号し、かつ、再生するための専用回路が必要であるため、従来の携帯電話機をそのまま用いて受信した暗号化音楽コンテンツデータを記録し、その記録された暗号化音楽コンテンツデータを復号および再生することはできない。

【0013】そこで、本発明は、かかる問題を解決するために必要なものであり、その目的は、従来の携帯電話機の構成を大幅に変更することなく、受信した暗号化音楽コンテンツデータを記録し、その記録された暗号化音楽コンテンツデータを復号および再生を行なうことができる携帯電話機およびそれに用いるアダプタを提供することである。

【0014】

【課題を解決するための手段および発明の効果】この発明による携帯電話機は、音楽データを暗号化した暗号化音楽データと、暗号化音楽データを復号して音楽データを復元するための復号鍵であるライセンス鍵とを記録したデータ記録装置から暗号化音楽データとライセンス鍵とを取得して音楽データを再生する携帯電話機であって、本体部と、本体部から脱着可能なアダプタとを備え、アダプタは、データ記録装置を脱着する着脱部と、データ端末装置を含み、データ端末装置は、データ記録装置とデータとの授受を行なうためのインタフェース部と、ライセンス鍵によって暗号化音楽データを復号して音楽データを復元する復号処理部と、復号処理部によって復元された音楽データから音楽を再生する音楽再生部と、制御部を含み、音楽データの再生時、制御部は、データ記録装置に記録された暗号化音楽データおよびライセンス鍵をインタフェース部を介して取得し、その取得した暗号化音楽データおよびライセンス鍵を前記復号処理部に与える。

【0015】この発明による携帯電話機においては、暗号化音楽データとライセンス鍵とを記録されたデータ記録装置がアダプタに装着された状態で、アダプタに含まれるデータ端末装置は、データ記録装置からライセンス鍵および暗号化音楽データを受取り、ライセンス鍵によって暗号化音楽データを復号し、再生する。

【0016】したがって、この発明によれば、暗号化音楽データの再生を、携帯電話機のアダプタにデータ記録装置を装着して行なうことができる。その結果、データ端末装置が含まれるアダプタを新規に装着するだけで携帯電話機の本体の構成を殆ど変更せずに暗号化音楽データの再生が可能である。

【0017】また、この発明による携帯電話機は、音楽データを暗号化した暗号化音楽データおよび/または暗号化音楽データを復号して音楽データを復元するための復号鍵であるライセンス鍵を受信してデータ記録装置に記録する携帯電話機であって、本体部と、アダプタとを備え、アダプタは、データ記録装置を脱着する着脱部

と、データ端末装置とを含み、データ端末装置は、データ記録装置とデータとの授受を行なうためのインタフェース部と、制御部とを含み、データの受信時、制御部は、本体部から暗号化音楽データおよび/またはライセンス鍵を受取り、その受取った暗号化音楽データおよび/またはライセンス鍵をインタフェース部を介してデータ記録装置に記録する。

【0018】この発明による携帯電話機においては、アダプタにデータ記録装置が装着された状態で、暗号化音楽データおよびライセンス鍵が本体側で受信され、アダプタ部のデータ端末装置へ送られる。そして、データ端末装置は、送られてきた暗号化音楽データとライセンス鍵とをデータ記録装置に記録する。

【0019】したがって、この発明によれば、暗号化音楽データのダウンロードを、携帯電話機のアダプタにデータ記録装置を装着して行なうことができる。その結果、データ端末装置が含まれるアダプタを新規に装着するだけで携帯電話機の本体の構成を殆ど変更せずに暗号化音楽データのダウンロードが可能である。

【0020】また、この発明による携帯電話機は、音楽データを暗号化した暗号化音楽データおよび/または暗号化音楽データを復号して音楽データを復元するための復号鍵であるライセンス鍵をデータ記録装置に記録し、またはデータ記録装置に記録された暗号化音楽データとライセンス鍵とを取得して音楽データを再生する携帯電話機であって、本体部と、アダプタとを備え、アダプタ部は、データ記録装置を脱着する着脱部と、データ端末装置を含み、データ端末装置は、データ記録装置とデータとの授受を行なうためのインタフェース部と、データ記録装置に対する認証データを保持する認証データ保持部と、ライセンス鍵によって暗号化音楽データを復号する復号処理部と、制御部を含み、データの受信時、制御部は、本体部から暗号化音楽データおよび/またはライセンス鍵を受取り、その受取った暗号化音楽データおよび/またはライセンス鍵をインタフェース部を介してデータ記録装置に記録し、データの再生時、制御部は、認証データをインタフェース部を介してデータ記録装置へ送り、データ記録装置において認証データが認証されることによってデータ記録装置から送られて来るライセンス鍵および暗号化音楽データを復号処理部へ入力する。

【0021】この発明による携帯電話機においては、アダプタにデータ記録装置が装着された状態で、暗号化音楽データおよびライセンス鍵が本体側で受信され、アダプタ部のデータ端末装置へ送られる。そして、データ端末装置は、送られてきた暗号化音楽データとライセンス鍵とをデータ記録装置に送る。データ記録装置は暗号化音楽データとライセンス鍵とを記録する。また、アダプタ部に含まれるデータ端末装置は、音楽データの再生時、データ記録装置に対する認証が終了した後にデータ

記録装置からライセンス鍵および暗号化音楽データを受取り、ライセンス鍵によって暗号化音楽データを復号し、再生する。

【0022】したがって、この発明によれば、暗号化音楽データのダウンロード、およびダウンロードした暗号化音楽データの再生を、携帯電話機のアダプタ部にデータ記録装置を装着して行なうことができる。その結果、データ端末装置に含まれるアダプタを新規に装着するだけで携帯電話機の本体の構成を殆ど変更せずに暗号化音楽データのダウンロード、およびダウンロードした暗号化音楽データの再生が可能である。

【0023】好ましくは、携帯電話機のアダプタ部は、データ端末装置から出力される音楽データの再生信号を外部出力装置へ出力するための音楽端子をさらに含む。

【0024】アダプタ部に含まれるデータ端末装置によって暗号化音楽データが復号、および再生されると、その再生された音楽データはアダプタに設けられた音楽端子に送られる。そして、音楽端子を介してヘッドホン等の外部出力装置へ音楽データが出力される。

【0025】したがって、この発明によれば、携帯電話機の本体に音楽データ専用の端子を新たに設けずにダウンロードした音楽を聴くことができる。

【0026】好ましくは、携帯電話機の本体部は、通話時に相手側から受取った音声信号を外部へ出力し、音声信号を入力するための音声端子を含む。

【0027】携帯電話機の本体側で受取られた相手側の音声信号は復調等されて本体に設けられた音声端子から外部へ出力される。また、アダプタ部に含まれるデータ端末装置によって復号および再生された音楽データはアダプタ部に設けられた音楽データ専用の音楽端子から外部へ出力される。

【0028】したがって、この発明によれば、従来の携帯電話機の構成を殆ど変更せずに、データ端末装置を含むアダプタを装着するだけでダウンロードされた音楽を専用端子から聴くことができる。

【0029】好ましくは、アダプタ部に設けられた音楽端子は、2チャンネルの出力信号を外部へ出力する。

【0030】音楽データ専用の音楽端子は、データ端末装置によって復号および再生された音楽データを2チャンネルの信号としてヘッドホン等の外部出力装置へ出力する。

【0031】したがって、携帯電話機ユーザは、ダウンロードした音楽をステレオによって聴くことができる。

【0032】好ましくは、携帯電話機の本体部は、データ端末装置から出力される音楽データの再生信号と、通話時に相手側から受取った音声信号とを外部出力装置へ出力し、音声信号を入力するための音楽音声端子を含む。

【0033】携帯電話機によって受信された音声信号、

およびデータ端末装置によって再生された音楽データは、本体に設けられた音楽音声端子を介して外部出力装置へ出力される。また、携帯電話機ユーザが話した音声信号は、音楽音声端子から携帯電話機へ取込まれ、相手側へ送信される。つまり、1つの端子を介して通常の通話、および音楽の再生が行なわれる。

【0034】したがって、この発明によれば、音楽を聴きながら通常の通話を行なうことができる。

【0035】好ましくは、携帯電話機の本体に設けられた音楽音声端子は、2チャンネルの出力信号を外部出力装置へ出力する。

【0036】携帯電話機の本体は、1つの端子を介して音声信号の入出力および音楽データの出力を行なう。そして、携帯電話機の本体は、音楽データを2チャンネルの出力信号としてヘッドホン等の外部出力装置へ出力する。

【0037】したがって、この発明によれば、ステレオで音楽を聴きながら通常の通話を行なうことができる。

【0038】好ましくは、携帯電話機のアダプタ部に含まれるデータ端末装置は、データ記録装置からライセンス鍵を取得するための第1のセッション鍵を発生するセッション鍵発生部と、バスに接続され、データ記録装置における認証データの認証に基づいて、データ記録装置から取得した第2のセッション鍵によって第1のセッション鍵を暗号化する暗号処理部とをさらに含む。復号処理部は、バスに接続され、第1のセッション鍵によって暗号化されたライセンス鍵を復号する第1の復号処理部と、バスに接続され、第1の復号処理部において復号されたライセンス鍵によって暗号化音楽データを復号する第2の復号処理部とから成り、データの再生時、制御部は、さらに、第2のセッション鍵を暗号処理部へ与え、第1のセッション鍵によって暗号化されたライセンス鍵を第1の復号処理部へ与え、暗号化音楽データを第2の復号処理部へ与える。

【0039】暗号化音楽データの再生時、データ端末装置は、データ端末装置に対する認証が終了した後、データ端末装置とデータ記録装置とにおいて発生されたセッション鍵によってデータ記録装置との間で相互認証を行ないながら、データ記録装置から暗号化音楽データおよびライセンス鍵を受取る。そして、データ端末装置は、ライセンス鍵によって暗号化音楽データを復号し、再生する。

【0040】したがって、この発明によれば、暗号化音楽データを正規のデータ端末装置によって再生することができる。その結果、携帯電話機を用いて暗号化音楽データを保護しながら音楽を楽しむことができる。

【0041】好ましくは、携帯電話機のアダプタ部に含まれるデータ端末装置は、バスに接続され、認証データに含まれる公開暗号鍵と非対称な秘密復号鍵を保持する鍵保持部と、バスに接続され、公開暗号鍵によって暗号

化された第2のセッション鍵を秘密復号鍵によって復号する第3の復号処理部とをさらに含み、データの再生時、制御部は、さらに、公開暗号鍵によって暗号化された第2のセッション鍵をデータ記録装置から受取り、第3の復号処理部へ与え、第3の復号処理部において復号された第2のセッション鍵を暗号処理部へ与える。

【0042】データ端末装置は、音楽データの再生時、公開鍵方式によってデータ記録装置において発生された第2のセッション鍵を受取る。そして、データ端末装置は、受取った第2のセッション鍵によって、自己が発生させた第1のセッション鍵を暗号化してデータ記録装置へ送り、第1のセッション鍵によって暗号化されたライセンス鍵をデータ記録装置から受取る。

【0043】したがって、この発明によれば、データ端末装置は秘密復号鍵を保持していれば良く、暗号化したデータのやり取りにおける鍵の管理が容易になる。また、この発明によれば、認証データによるデータ端末装置のデータ記録装置に対する認証、およびセッション鍵によるデータ端末装置とデータ記録装置との相互認証という2重のセキュリティによって暗号化音楽データを保護できる。

【0044】好ましくは、携帯電話機の本体部は、アダプタ部に含まれるデータ端末装置を駆動する駆動電源を含む。

【0045】携帯電話機に備えられた駆動電源からデータ端末装置を駆動するための駆動電力が供給される。したがって、この発明によれば、データ端末装置を含むアダプタのみを装着することによって従来の携帯電話機の構成を殆ど変更せずに暗号化音楽データをダウンロードでき、そのダウンロードした暗号化音楽データを復号および再生できる。

【0046】好ましくは、アダプタ部は、データ端末装置を駆動する駆動電源をさらに含む。

【0047】アダプタ部に含まれるデータ端末装置は、アダプタ部に含まれる駆動電源によって駆動され、暗号化音楽データの再生等を行なう。したがって、この発明によれば、暗号化音楽データのダウンロード、および復号・再生を行なうための電力と携帯電話機の本体を駆動するための電力とを賄う駆動電源をアダプタ部に設けることによって、従来の携帯電話機の構成を殆ど変更せずに暗号化音楽データのダウンロード、および復号・再生を行なうことができる。

【0048】また、この発明によるアダプタは、音楽データを暗号化した暗号化音楽データと、暗号化音楽データを復号して音楽データを復元するための復号鍵であるライセンス鍵とを記録したデータ記録装置から暗号化音楽データとライセンス鍵とを取得して音楽データを再生する携帯電話機に装着するアダプタであって、データ記録装置を脱着する着脱部と、データ端末装置とを備え、データ端末装置は、データ記録装置とデータの授受を行

なうためのインタフェース部と、データ記録装置に対する認証データを保持する認証データ保持部と、ライセンス鍵によって暗号化音楽データを復号する復号処理部と、制御部とを含み、音楽データの再生時、制御部は、認証データをインタフェース部を通じてデータ記録装置へ送り、データ記録装置において認証データが認証されることによってデータ記録装置から送られてくるライセンス鍵および暗号化音楽データを受取り、その受取った暗号化音楽データおよびライセンス鍵を復号処理部に与える。

【0049】この発明によるアダプタにおいては、暗号化音楽データおよびライセンス鍵が記録されたデータ記録装置が装着された状態で、アダプタに含まれるデータ端末装置は、データ記録装置に対する認証が終了した後、データ記録装置からライセンス鍵および暗号化音楽データを受取り、ライセンス鍵によって暗号化音楽データを復号し、再生する。

【0050】したがって、この発明によれば、暗号化音楽データの再生を携帯電話機のアダプタにデータ記録装置を装着して行なうことができる。その結果、携帯電話機のユーザは、データ端末装置が含まれるアダプタを新規に購入するだけで、携帯電話機を用いて暗号化音楽データの再生を行なうことができる。

【0051】また、この発明によるアダプタは、音楽データを暗号化した暗号化音楽データおよび/または暗号化音楽データを復号して音楽データを復元するための復号鍵であるライセンス鍵を受信してデータ記録装置に記録する携帯電話機に装着するアダプタであって、データ記録装置を脱着する着脱部と、データ端末装置とを備え、データ端末装置は、データ記録装置とデータの授受を行なうためのインタフェース部と、制御部とを含み、データの受信時、制御部は、携帯電話機から暗号化音楽データおよび/またはライセンス鍵を受取り、その受取った暗号化音楽データおよび/またはライセンス鍵をインタフェース部を通じてデータ記録装置に記録する。

【0052】この発明によるアダプタにおいては、データ記録装置が装着された状態で、携帯電話機の本体側で受信された暗号化音楽データおよびライセンス鍵が力入れされる。そして、アダプタに含まれるデータ端末装置は、入力された暗号化音楽データとライセンス鍵とをデータ記録装置に送る。データ記録装置は暗号化音楽データとライセンス鍵とを記録する。

【0053】したがって、この発明によれば、暗号化音楽データのダウンロードを、携帯電話機のアダプタにデータ記録装置を装着して行なうことができる。その結果、携帯電話機のユーザは、データ端末装置が含まれるアダプタを新規に購入するだけで、携帯電話機を用いて暗号化音楽データのダウンロードを行なうことができる。

【0054】また、この発明によるアダプタは、音楽デ

ータを暗号化した暗号化音楽データおよび/または暗号化音楽データを復号して音楽データを復元するための復号鍵であるライセンス鍵とを受信してデータ記録装置に記録し、またはデータ記録装置に記録された暗号化音楽データとライセンス鍵とを取得してデータを再生する携帯電話機に装着するアダプタであって、データ記録装置を着脱するための着脱部と、データ端末装置とを備え、データ端末装置は、データ記録装置にデータの授受を行なうためのインタフェース部と、データ記録装置に対する認証データを保持する認証データ保持部と、ライセンス鍵によって暗号化音楽データを復号する復号処理部と、制御部とを含み、データの受信時、制御部は、携帯電話機から暗号化音楽データおよび/またはライセンス鍵を受取り、その受取った暗号化音楽データおよび/またはライセンス鍵をインタフェース部を介してデータ記録装置に記録し、データの再生時、制御部は、認証データをインタフェース部を介してデータ記録装置へ送り、データ記録装置において認証データが認証されることによってデータ記録装置から送られてくるライセンス鍵および暗号化音楽データを受取り、その受取ったライセンス鍵および暗号化音楽データを復号処理部へ入力する。

【0055】この発明によるアダプタにおいては、データ記録装置が装着された状態で、携帯電話機の本体側で受信され暗号化音楽データおよびライセンス鍵が入力される。そして、アダプタに含まれるデータ端末装置は、入力された暗号化音楽データとライセンス鍵とをデータ記録装置に送る。データ記録装置は暗号化音楽データとライセンス鍵とを記録する。また、アダプタに含まれるデータ端末装置は、音楽データの再生時、データ記録装置に対する認証が終了した後データ記録装置からライセンス鍵および暗号化音楽データを受取り、ライセンス鍵によって暗号化音楽データを復号し、再生する。

【0056】したがって、この発明によれば、暗号化音楽データのダウンロード、およびダウンロードした暗号化音楽データの再生を、携帯電話機のアダプタにデータ記録装置を装着して行なうことができる。その結果、携帯電話機のユーザは、データ端末装置が含まれるアダプタを新規に購入するだけで、携帯電話機を用いて暗号化音楽データのダウンロードし、かつ、ダウンロードした暗号化音楽データの再生を行なうことができる。

【0057】好ましくは、アダプタは、データ端末装置から出力される音楽データの再生信号を外部出力装置へ出力するための音楽端子をさらに含む。

【0058】アダプタに含まれるデータ端末装置によって暗号化音楽データが復号、および再生されると、その再生された音楽データはアダプタに設けられた音楽端子に送られる。そして、音楽端子を介してヘッドホン等の外部出力装置へ音楽データが出力される。

【0059】したがって、この発明によれば、携帯電話機の本体に音楽データ専用の端子を新たに設けずにダウ

ンロードした音楽を聴くことができる。

【0060】好ましくは、アダプタはデータ端末装置の駆動電源をさらに備える。アダプタに含まれるデータ端末装置は、アダプタに含まれる駆動電源によって駆動され、暗号化音楽データの再生等を行なう。したがって、この発明によれば、暗号化音楽データのダウンロード、および復号・再生を行なうための電力と携帯電話機の本体を駆動するための電力とを結ぶ駆動電源をアダプタに設けることによって、従来の携帯電話機の構成を殆ど変更せずに暗号化音楽データのダウンロード、および復号・再生を行なうことができる。

【0061】好ましくは、アダプタは携帯電話機に対して駆動電源を供給する。アダプタは、通常の電話機能を果たす携帯電話機に駆動電源を供給する。

【0062】したがって、この発明によれば、従来の電話機能を果たす携帯電話機にアダプタを装着することによって暗号化音楽データを再生することができる。

【0063】好ましくは、アダプタは、携帯電話機から駆動電源の供給を受け、アダプタは、装着された携帯電話機から駆動電源の供給を受け、暗号化音楽データを再生する。

【0064】したがって、この発明によれば、従来の携帯電話機にアダプタを装着するだけで暗号化音楽データを再生することができる。

【0065】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0066】【実施の形態1】図1は、本発明による携帯電話機が再生の対象とする暗号化コンテンツデータをメモリカードへ配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0067】図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得た、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバに中継する。著作権の存在する音楽データを管理するライセンスサーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機100に装着されたメモリカード110が正当な認証データを持つ与否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化し、データ配信を求めた配信キャリア20である携帯電話会社、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてライセンスを与える。

【0068】配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100に装着されたメモリカード110に対して、携帯電話網および携帯電話機100を介して暗号化コンテンツデータとライ

ンスとを配信する。

【0069】図1においては、たとえば携帯電話ユーザの携帯電話機100には、着脱可能なメモ리카ード110が装着される。メモ리카ード110は、携帯電話機100により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化については復号した上で、携帯電話機100中の音楽再生回路(図示せず)に与える。

【0070】さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【0071】以下では、このようなライセンスサーバ10と配信キャリア20と併せて、配信サーバ30と総称することとする。

【0072】また、このような配信サーバ30から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【0073】このような構成とすることで、まず、メモ리카ード110を利用しないと、配信サーバ30からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0074】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信(ダウンロード)するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0075】図1に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話のユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号鍵を配信するための方式であり、さらに第2には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【0076】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置および音楽再生回路(携帯電話機)に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0077】図2を参照して、この発明による携帯電話機100の外観について説明する。図2は、携帯電話機100の裏面を示したものである。携帯電話機100は、アダプタ140と、結合端子1118、1224とを含む。アダプタ140は、メモ리카ード110を着脱

するための着脱部1226と、暗号化音楽データを復号および再生して聴くためのヘッドホン130を接続するためのジャック1220とを備える。結合端子1118、1224は、携帯電話機100の本体105とアダプタ140とを接続する。したがって、後述するように、配信サーバ30からの暗号化音楽データの配信においては、結合端子1224を介して、暗号化音楽データ等がやり取りされる。また、後述するようにアダプタ140はバッテリーを含むため、携帯電話機100の本体105の駆動電力は結合端子1118を介して本体105へ供給される。

【0078】さらに、アダプタ140は本体105から着脱可能であり、すでに販売されている携帯電話機に駆動電力を供給するバッテリーアダプタを交換して装着可能な構造になっている。したがって、メモ리카ード110の着脱部1226、および後述する暗号化音楽データを復号・再生するための機能と必要とするユーザのみが、アダプタ140だけを購入して、自己の携帯電話機にアダプタ140を装着すれば、配信サーバ30から希望する暗号化音楽データをダウンロードし、かつ、暗号化音楽データを復号・再生できる。

【0079】図3を参照して、携帯電話機100は、本体105と、アダプタ140とから成る。本体105は、アンテナ1102と、マイクロコンピュータユニット(MCU)1106と、音声コーデック1112と、スピーカ1111と、マイク1113と、ジャック1114と、パッド1116とを含む。MCU1106は、データバスBS2を介してパッド1116と接続される。また、MCU1106は、データバスBS2と独立なデータバスBS3Aおよび結合端子1224を介してアダプタ140に接続される。

【0080】アンテナ1102は、通常の電話機能においては、相手側の音声信号を受信し、その受信した音声信号をMCU1106へ与える。また、携帯電話機100のユーザが話した音声信号を相手の電話へ送信する。また、アンテナ1102は、配信サーバ30から暗号化音楽データをダウンロードするときは、配信サーバ30との間でデータを送受信する。

【0081】MCU1106は、携帯電話機100の通常の電話機能等を制御する。音声コーデック1112は、通常の電話機能において相手側の音声信号をMCU1106から受取り、その受取った音声信号を復調し、デジタル信号からアナログ信号へ変換してスピーカ1111またはジャック1114へ出力し、データバスBS2を介してパッド1116へ、さらにデータバスBS3Aと結合端子1224を介してアダプタ140へ出力する。また、音声コーデック1112は、携帯電話機100のユーザが話した音声データをマイク1113、ジャック1114またはデータバスBS2を介してパッド1116から受取り、その受取った音声データをアナロ

グ信号からデジタル信号へ変換し、所定の方式に変調してMCU1108へ与える。

【0082】ジャック1114は、イヤホンマイク（図示せず）に接続可能な端子であり、音声コーデック1112によって復調等された音声データをイヤホンマイクへ出力する。また、ジャック1114は、携帯電話機100のユーザが話した音声データをイヤホンマイクを介して受取り、音声コーデック1112へ出力する。なお、ジャック1114は、モノラルの音声データを出力する。

【0083】パッド1116は、外部インタフェースと内部インタフェースを含み、外部からの制御コマンドを外部インタフェースを介して内部インタフェースへ引込む。また、パッド1116はマイク（図示せず）またはイヤホン（図示せず）と接続され、音声コーデック1112によって復調等された音声データをデータバスB52を介して受取り、パッド1116を介してイヤホンへ出力するとともに、携帯電話機100のユーザが話した音声データをパッド1116を介して、マイクから受取り、バスB52を介して音声コーデック1112へ出力する。

【0084】アダプタ140は、データ端末装置120と、バッテリー150と、ジャック1220とを含む。バッテリー150は、データ端末装置120へ駆動電力を供給するとともに、本体105へ結合端子1118を介して駆動電力を供給する。バッテリー150は、メモリアカード1110から暗号化音楽データを読み出して復号および再生を行なうデータ端末装置120を駆動するための電源、および本体105のMCU1108等を駆動するための電源として機能するため、アダプタ140に含まれる。すなわち、バッテリー150は、メモリアカード1110からの暗号化音楽データの読み出し、復号、および再生という特殊機能を有するデータ端末装置120も含め、携帯電話機100全体の駆動電力を供給する必要があるため、アダプタ140に新設したものである。これによって、ユーザはアダプタ140のみを購入して、携帯電話機のバッテリーアダプタと交換して装着できる。その結果、ユーザは、メモリアカード1110への暗号化音楽データのダウンロードおよび復号・再生を容易に行なうことができる。

【0085】ジャック1220は、本体105の音声コーデック1112によって復調等された音声データをデータ端末装置120を介して受取り、接続されたヘッドホン130へ出力する。また、ジャック1220は、データ端末装置120によって復号および再生された音楽データを接続されたヘッドホン130へ出力する。なお、ジャック1220は、2チャンネルの音声データを出力する。

【0086】データ端末装置120は、公開鍵復号部1206と、DES1214と、MP3デコーダ1216

と、DAC1218と、MCU1222と、共通鍵暗号・復号部1230を含む。データバスB53Bは、結合端子1224を介して本体105のデータバスB53Aと接続される。すなわち、本体105のMPU1106とアダプタ140のMPUは、データバスB53A、結合端子1224およびデータバスB53Bを介して接続される。以降、結合端子1224で接続されたデータバスB53AおよびデータバスB53Bを総称してデータバスB53と称する。

10 【0087】MCU1222は、配信サーバ30からの暗号化音楽データの配信時、着脱部1226に装着されたメモリアカード110からのデータ等を結合端子1224およびバスB53を介して本体105のMCUへ出力するとともに、本体105のMCU1108からのデータ等をメモリアインタフェースを介してメモリアカード110へ出力する。

【0088】また、MCU1222はメモリアカード110からの暗号化音楽データを復号および再生するとき、メモリアカード110からのデータ等を公開鍵復号部1206、共通鍵暗号・復号部1230へ入出力するとともに、暗号化音楽データと、その暗号化音楽データを復号するためのライセンス鍵をDES1214へ与える。

【0089】公開鍵復号部1206は、後述するように公開鍵による復号処理を行なう。共通鍵暗号・復号部1230は、後述するように共通鍵による暗号処理および復号処理を行なう。

【0090】DES1214は、ライセンス鍵によって暗号化音楽データを復号する。MP3デコーダ1216は、MP3（MPEG1オーディオ・レイヤ3）方式によって圧縮された音楽データを解凍して再生する。

30 【0091】DAC1218は、MP3デコーダ1216によって解凍して再生された音楽データをデジタル信号からアナログ信号へ変換する。

【0092】上述したようにアダプタ140は、配信サーバ30からダウンロードした暗号化音楽データを記録するためにメモリアカード110へ与え、暗号化音楽データをメモリアカード110から読み出して復号および再生するためのデータ端末装置120と、データ端末装置120と、本体105の各部とに電力を供給するバッテリー150を含む。

40 【0093】以下、携帯電話機100を用いた配信サーバ30からの暗号化音楽データの配信、およびその配信された暗号化音楽データの復号・再生について説明する。

【0094】図4は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。ここでは、MP3方式によって符号化された音楽データを再生するための構成を示しているが、音楽データの圧縮方式を規定するものではなく、他の符号化方式によって符号化された音楽データに

いてはMP3デコーダ1216に代えて、音楽データを符号化した復号化方式に適したデコーダを配置すれば実現可能である。

【0095】まず、配信サーバ30より配信されるデータについて説明する。携帯電話機100に配信されるべきDataは、MP3方式によって符号化された音楽データから成るコンテンツデータである。コンテンツデータDataには、ライセンス鍵Kcで復号可能な暗号化が施される。ライセンス鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータ(Data)Kcがこの形式で配信サーバ30より携帯電話ユーザに配布される。

【0096】なお、以下においては、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0097】さらに、配信サーバ30からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報DataInfが配布される。また、ライセンス情報としては、コンテンツデータDataを識別するためのコードであるコンテンツIDおよびライセンスの発行を特定できる管理コードであるライセンスIDや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置(メモリカード)のアクセスに対する制限に関する情報であるアクセス制限情報AC1およびデータ端末装置(携帯電話機またはアダプタ)における制御情報である再生回路制御情報AC2等が存在する。以後、ライセンス鍵KcとコンテンツIDとライセンスIDとアクセス制御情報AC1と再生回路制御情報AC2とを併せて、ライセンスと総称することとする。

【0098】図5は、図1に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【0099】本発明の実施の形態1においては、記録装置(メモリカード)やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および再生を禁止することができるよう禁止クラスリストCRL(Class Revocation List)の運用を行なう。以下では、必要に応じて記号CRLによって禁止クラスリスト内のデータを表わすこともある。

【0100】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止されるデータ端末装置およびメモリカードのクラスをリストアップした禁止クラスリストデータCRLが含まれる。

【0101】禁止クラスリストデータCRLは、配信サーバ30内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時

バージョンアップしデータを更新していく必要があるが、データの更新については、基本的には変更点のみを反映した差分データCRL_dataを配信サーバ30側より発生して、これに応じてメモリカード内の禁止クラスリストCRLが書き換えられる構成とする。また、禁止クラスリストのバージョンについては、CRL_verをメモリカード側より出力し、これを配信サーバ30側で確認することによってバージョン管理を実行する。差分データCRL_dataには新たなバージョンの情報も含まれる。また、バージョン情報として、更新日時を用いることも可能である。

【0102】このように、禁止クラスリストCRLを、配信サーバのみならずメモリカード内においても保持運用することによって、クラス固有すなわち、データ端末装置およびメモリカードの種類の復号鍵が破られた、データ端末装置およびメモリカードへのライセンス鍵の供給が禁止される。このため、データ端末装置ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

【0103】このように、メモリカード内の禁止クラスリストCRLは配信時に逐次データを更新する構成とする。また、メモリ回路内における禁止クラスリストCRLの管理は、上位レベルとは独立にメモリカード内でタンパーレジスタントモジュール(Tamper Resistance Module)に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータCRLを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとなることが

【0104】データ端末装置およびメモリカードには固有の公開暗号鍵Kp nおよびKp m c i がそれぞれ設けられ、公開暗号鍵Kp nおよびKp m c i は携帯電話機に固有の秘密復号鍵K m c i およびメモリカード固有の秘密復号鍵K m c i によってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、データ端末装置の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【0105】また、暗号化音楽データを再生するデータ端末装置およびメモリカードのクラス証明書として、C r t f n およびC m c i がそれぞれ設けられる。

【0106】これらのクラス証明書は、データ端末装置およびメモリカードのクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【0107】これらのコンテンツ再生装置およびメモリカードのクラス固有の公開暗号鍵およびクラス証明書

は、認証データ {K P p n / / C r t f n} K P m a および {K P m c i / / C m c i} K P m a の形式で、出荷時にデータ端末装置を搭載した携帯電話機およびメモリカードにそれぞれ記録される。また、データ端末装置 120 を含むアダプタ 140 を単独で出荷する場合は、証明書は上記の認証データの形式で出荷時にアダプタ 140 のデータ端末装置 120 に記録される。後ほど詳細に説明するが、K P m a は配信システム全体で共通の公開認証鍵である。

【0108】図 8 は、図 1 に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

【0109】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ 30、データ端末装置 120、メモリカード 110 において生成される共通鍵 K s 1 ~ K s 3 が用いられる。

【0110】ここで、共通鍵 K s 1 ~ K s 3 は、配信サーバ、データ端末装置もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵 K s 1 ~ K s 3 を「セッションキー」とも呼ぶこととする。

【0111】これらのセッションキー K s 1 ~ K s 3 は、各通信セッションごとに固有の値を有することにより、配信サーバ、データ端末装置およびメモリカードによって管理される。具体的には、セッションキー K s 1 は、配信サーバによって配信セッションごとに発生される。セッションキー K s 2 は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキー K s 3 は、データ端末装置において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0112】また、メモリカード 110 内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵 K P m 2、公開暗号鍵 K P m で暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵 K m が存在する。

【0113】図 7 は、図 1 に示したライセンスサーバ 100 の構成を示す概略ブロック図である。

【0114】ライセンスサーバ 100 は、コンテンツデータを所定の方法に従って暗号化したデータや、ライセンス ID 等の配信情報を保持するための情報データベース 304 と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金

データベース 302 と、禁止クライアント CRL を管理する CRL データベース 306 と、情報データベース 304、課金データベース 302 および CRL データベース 306 からのデータをデータベース B S 1 を介して受取り、所定の処理を行なうためのデータ処理部 310 と、通信線を介して、配信キャリア 20 とデータ処理部 310 との間でデータ授受を行なうための通信装置 350 とを備える。

【0115】データ処理部 310 は、データベース B S 1 上のデータに応じて、データ処理部 310 の動作を制御するための配信制御部 315 と、配信制御部 315 に制御されて、配信セッション時にセッションキー K s 1 を発生するためのセッションキー発生部 316 と、メモリカードから携帯電話機を介して送られてきた認証のための認証データ {K P m c i / / C m c i} K P m a を通信装置 350 およびデータベース B S 1 を介して受けて、公開認証鍵 K P m a による復号処理を行なう復号処理部 312 と、セッションキー発生部 316 より生成されたセッションキー K s 1 を復号処理部 312 によって得られた公開暗号鍵 K P m c m を用いて暗号化して、データベース B S 1 に出力するための暗号化処理部 318 と、セッションキー K s 1 によって暗号化された上で送信されたデータをデータベース B S 1 より受けて、復号処理を行なう復号処理部 320 とを含む。

【0116】データ処理部 310 は、さらに、配信制御部 315 から与えられるライセンス鍵 K c o および再生回路制御情報 A C 2 を、復号処理部 320 によって受けたメモリカード固有の公開暗号鍵 K P m によって暗号化するための暗号化処理部 326 と、暗号化処理部 326 の出力を、復号処理部 320 から与えられるセッションキー K s 2 によってさらに暗号化してデータベース B S 1 に出力するための暗号化処理部 328 とを含む。

【0117】ライセンスサーバ 100 の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0118】図 8 は、図 3 に示した携帯電話機 100 の本体 105 の構成をさらに詳細に説明するための概略ブロック図である。

【0119】携帯電話機 100 の本体 105 は、アンテナ 1102 からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機 100 のデータを変調してアンテナ 1102 に与えるための送受信部 1104 と、外部からの指示を携帯電話機 100 に与えるためのキー操作部 1108 と、MCU 1106 等から出力される情報を携帯電話機ユーザに視覚情報として与えるためのディスプレイ 1110 とを、図 3 の構成に追加して含む。

【0120】なお、図 8 においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一

部図記載を省略している。

【0121】図9は、図3に示したデータ端末装置120の概略ブロックを詳細に示したものである。データ端末装置120は、配信サーバ30からのコンテンツデータ（音楽データ）を記憶しつつ復号化処理するための着脱可能なメモリカード110と、メモリカード110とデータバスBS3との間のデータの授受を制御するためのメモリインタフェース1200とをさらに含む。

【0122】データ端末装置120は、また、携帯電話機の種別（クラス）ごとにそれぞれ設定される、公開暗号鍵K_{Pp1}およびクラス証明書C_{rtf1}を公開復号鍵K_{Pma}で復号することでその正当性を認証できる状態に暗号化した認証データ{K_{Pp1}//C_{rtf1}}K_{Pma}を保持する認証データ保持部1202をさらに含む。ここで、携帯電話機（コンテンツ再生回路）100のクラスnは、n=1であるとする。

【0123】データ端末装置120は、さらに、データ端末装置に固有の復号鍵であるK_{p1}を保持するK_{p1}保持部1204と、データバスBS3から受けたデータをK_{p1}によって復号しメモリカード110によって発生されたセッションキーK_{s2}を得る復号処理部1205とをさらに含む。K_{p1}保持部1204と復号処理部1205とは図3に示す公開鍵復号部1208に相当する。

【0124】データ端末装置120は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行う再生セッションにおいてメモリカード110との間でデータバスBS3上においてやり取りされるデータを暗号化するためのセッションキーK_{s3}を乱数等により発生するセッションキー発生部1210と、生成されたセッションキーK_{s3}を復号処理部1205によって得られたセッションキーK_{s2}によって暗号化し、データバスBS3に出力する暗号化処理部1208を含む。

【0125】データ端末装置120は、さらに、データバスBS3上のデータをセッションキーK_{s3}によって復号して出力する復号処理部1212を含む。暗号処理部1208、セッションキー発生部1210、および復号処理部1212は、図3に示す共通暗号部・復号部1230に相当する。

【0126】データ端末装置120は、さらに、データバスBS3より暗号化コンテンツデータ{Data}K_cを受けて、復号処理部1212からバスBS3を介して取得したライセンス鍵K_cによって復号し、コンテンツデータを出力する復号処理部1214と、復号処理部1214の出力を受けてコンテンツデータを解凍して再生するためのMP3デコーダ1216と、MP3デコーダ1216の出力をデジタル信号からアナログ信号に変換するとともに、携帯電話機100の本体105からバスBS3を介して入力された音声データをミックスするDAC1218を含む。

【0127】図10は、メモリカード110の構成を説明するための概略ブロック図である。

【0128】既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、K_{Pmc1}およびK_{mc1}が設けられ、メモリカードのクラス証明書C_{mc1}が設けられるが、メモリカード110においては、これらは自然数i=1でそれぞれ表わされるものとする。

【0129】したがって、メモリカード110は、認証データ{K_{Pmc1}//C_{mc1}}K_{Pma}を保持する認証データ保持部1400と、メモリカードの種類ごとに設定される固有の復号鍵であるK_{mc1}を保持するK_{mc}保持部1402と、メモリカードごとに固有に設定される秘密復号鍵K_{m1}を保持するK_{m1}保持部1421と、K_{m1}によって復号可能な公開暗号鍵K_{Pm1}を保持するK_{Pm1}保持部1416とを含む。認証データ保持部1400は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵K_{Pmc1}およびクラス証明書C_{mc1}を公開認証鍵K_{Pma}で復号することでその正当性を認証できる状態に暗号化した認証データ{K_{Pmc1}//C_{mc1}}K_{Pma}ととして保持する。

【0130】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかにするように、配信されたコンテンツデータやライセンスの管理をメモリカード単位で実行することが可能になる。

【0131】メモリカード110は、さらに、メモリインタフェース1200との間で信号を端子1201を介して授受するデータバスBS4と、データバスBS4にメモリインタフェース1200から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵K_{mc1}をK_{mc1}保持部1402から受けて、配信サーバ30が配信セッションにおいて生成したセッションキーK_{s1}を拠点Paに出力する復号処理部1404と、K_{Pma}保持部1414から認証鍵K_{Pma}を受けて、データバスBS4に与えられるデータからK_{Pma}による復号処理を実行して復号結果を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1444によって選択的に与えられるデータを暗号化してデータバスBS4に出力する暗号化処理部1406とを含む。

【0132】メモリカード110は、さらに、配信、および再生の各セッションにおいてセッションキーK_{s2}を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーK_{s2}を復号処理部1408によって得られる公開暗号鍵K_{Pn}もしくは他のメモリカードの公開暗号鍵K_{Pmc1}によって暗号化してデータバスBS4に送出する暗号化

処理部1410と、データバスBS4よりセッションキーKs2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーKs2によって復号し、復号結果をデータバスBS5に送出する復号処理部1412を含む。

【0133】メモリアード110は、さらに、データバスBS4上のデータを公開暗号鍵Kpmlと対をなすメモリアード110固有の秘密暗号鍵Km1によって復号するための復号処理部1422と、禁止クラスリストのバージョン更新のためのデータCRL_dataによって逐次更新される禁止クラスリストデータCRLをデータバスBS5より受けて格納するとともに、暗号化コンテンツデータ(Data)Kcおよび付加情報Data_infをデータバスBS4より受けて格納するためのメモリアード115を含む。メモリアード115は、例えば半導体メモリによって構成される。

【0134】メモリアード110は、さらに、復号処理部1422によって得られるライセンスを保持するためのライセンス情報保持部1440と、データバスBS4を介して外部との間でデータ授受を行ない、データバスBS5との間で再生情報等を受けて、メモリアード110の動作を制御するためのコントローラ1420を含む。

【0135】ライセンス情報保持部1440は、N個(N:自然数)のバンクを有し、各暗号化コンテンツに対するライセンスをバンクごとに保持する。

【0136】なお、図10において、実線が囲んだ領域は、メモリアード110内において、外部からの不当な開封処理等が行なわれず、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれているものとする。このようなモジュールは、一般にはタンパレジスタンスモジュール(Tamper Resistance Module)である。

【0137】もちろん、メモリアード115も含めて、モジュールTRM内に組込まれる構成としてもよい。しかしながら、図10に示したような構成とすることで、メモリアード115中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリアード115中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパレジスタンスモジュール内にメモリアード115を設ける必要がないので、製造コストが低減されるという利点がある。

【0138】次に、図1に示すデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

【0139】図11および図12は、図1に示すデータ配信システムにおけるコンテンツの購入時に発生する配信動作(以下、配信セッションという)を説明するた

めの第1および第2のフローチャートである。

【0140】図11および図12においては、携帯電話ユーザが、メモリアード110を用いることで、携帯電話機100を介して配信サーバ30から音楽データであるコンテンツデータの配信を受ける場合の動作を説明している。

【0141】まず、携帯電話ユーザの携帯電話機100から、携帯電話ユーザによるキー操作部1108のキーボタンの操作等によって、配信リクエストがなされる(ステップS100)。

【0142】そうすると、携帯電話機100のMCU1106は、配信リクエストがなされたことをバスBS3および結合端子1224を介してデータ端末装置120のMCU1222へ出力する。そして、MCU1222は、配信リクエストをモジュールファースト200を介してメモリアード110へ出力する。メモリアード110においては、この配信リクエストに応じて、認証データ保持部1400より認証データ(KPmc1//Cmc1)KPmaが出力される(ステップS102)。

【0143】データ端末装置120は、メモリアード110から受理した認証データ(KPmc1//Cmc1)KPmaを結合端子1224およびバスBS3を介して携帯電話機100へ出力する。携帯電話機100は、メモリアード110からの認証のための認証データ(KPmc1//Cmc1)KPmaに加えて、コンテンツID、ライセンス購入条件のデータACとを配信サーバ30に対して送信する(ステップS104)。

【0144】配信サーバ30では、携帯電話機100からコンテンツID、認証データ(KPmc1//Cmc1)KPma、ライセンス購入条件データACを受信し(ステップS106)、復号処理部312においてメモリアード110から出力された認証データを公開認証鍵KPmaで復号処理を実行する(ステップS108)。

【0145】配信制御部315は、復号処理部312における復号処理結果から、処理が正常に行われたか否か、すなわち、メモリアード110が正規のメモリアードからの公開暗号鍵KPmc1と証明書Cmc1を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行う(ステップS110)。正当な認証データであると判断された場合、配信制御部315は、公開暗号鍵KPmc1および証明書Cmc1を承認し、受理する。そして、次の処理(ステップS12)へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵KPmc1および証明書Cmc1を受理しないので処理を終了する(ステップS170)。

【0146】認証の結果、正規の機器であることが認識されると、配信制御部315は、次に、メモリアード110のクラス証明書Cmc1が禁止クラスリストCRL

にリストアップされているかどうかをCRLデータベース306に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する(ステップS170)。

【0147】一方、メモリカード110のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する(ステップS112)。

【0148】認証の結果、正当な認証データを持つメモリカードを備えるリモコンおよび携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ30において、セッションキー発生部316は、配信のためのセッションキーKs1を生成する。セッションキーKs1は、復号処理部312によって得られたメモリカード110に対応する公開暗号鍵Kpmlによって、暗号化処理部318によって暗号化される(ステップS114)。

【0149】暗号化されたセッションキーKs1は、[Ks1]Kmc1として、データバスBS1および通信装置350を介して外部に出力される(ステップS116)。

【0150】携帯電話機100が、暗号化されたセッションキー(Ks1)Kmc1を受信すると(ステップS118)、メモリカード110においては、メモリインタフェース1200を介して、データバスBS4に与えられた受信データを、復号処理部1404が、保持部1402に保持されるメモリカード110固有の秘密復号鍵Kmc1により復号処理することにより、セッションキーKs1を復号し抽出する(ステップS120)。

【0151】コントローラ1420は、配信サーバ30で生成されたセッションキーKs1の受信を確認すると、セッションキー発生部1418に対して、メモリカード110において配信動作時に生成されるセッションキーKs2の生成を指示する。

【0152】また、配信セッションにおいては、コントローラ1420は、メモリカード110内のメモリ1415に記録されている禁止クラスリストの状態(バージョン)に関連する情報として、リストのバージョンデータCRL_verをメモリ1415から抽出してデータバスBS5に出力する。

【0153】暗号化処理部1406は、切換スイッチ1442の接点Paを介して復号処理部1404より与えられるセッションキーKs1によって、切換スイッチ1444および1446の接点を順次切換えることによって与えられるセッションキーKs2、公開暗号鍵Kpmlおよび禁止クラスリストのバージョンデータCRL_verを1つのデータ列として暗号化して、{Ks2//Kpml//CRL_ver}Ks1をデータバスBS4に出力する(ステップS122)。

【0154】データバスBS4に出力された暗号化データ{Ks2//Kpml//CRL_ver}Ks1

は、データバスBS4から端子1201およびメモリインタフェース1200を介してデータ端末装置120に出力され、データ端末装置120から結合端子1224およびバスBS3を介して携帯電話機100へ出力され、携帯電話機100から配信サーバ30に送信される(ステップS124)。

【0155】配信サーバ30は、暗号化データ{Ks2//Kpml//CRL_ver}Ks1を受信して、復号処理部320においてセッションキーKs1による復号処理を実行し、メモリカード110で生成されたセッションキーKs2、メモリカード110固有の公開暗号鍵Kpmlおよびメモリカード110における禁止クラスリストのバージョンデータCRL_verを受理する(ステップS126)。

【0156】禁止クラスリストのバージョン情報CRL_verは、データバスBS1を介して配信制御部315に送られ、配信制御部315は、受理したバージョンデータCRL_verに従って、当該CRL_verのバージョンとCRLデータベース306内の禁止クラスリストデータの現在のバージョンとの間の変化を表わす差分データCRL_datを生成する(ステップS128)。

【0157】さらに、配信制御部315は、ステップS106で取得したコンテンツIDおよびライセンス購入条件データACに従って、ライセンスID、アクセス制限情報AC1および再生回路制御情報AC2を生成する(ステップS130)。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Kcを情報データベース304より取得する(ステップS132)。

【0158】図12を参照して、配信制御部315は、生成したライセンス、すなわち、ライセンス鍵Kc、再生回路制御情報AC2、ライセンスID、コンテンツID、およびアクセス制限情報AC1を暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたメモリカード110固有の公開暗号鍵Kpmlによってライセンスを暗号化する(ステップS136)。暗号化処理部328は、暗号化処理部326の出力と、配信制御部315がデータバスBS1を介して供給する禁止クラスリストの差分データCRL_datとを受けて、メモリカード110において生成されたセッションキーKs2によって暗号化する。暗号化処理部328より出力された暗号化データは、データバスBS1および通信装置350を介して携帯電話機100に送信される(ステップS138)。

【0159】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向

上させることができる。

【0160】携帯電話機100は、送信された暗号化データ { [Kc//AC2//ライセンスID//コンテンツID//AC1] Km1//CRL_dat } Ks2を受信し(ステップS140)。MCU1106は、バスBS3および結合端子1224を介して暗号化データ { [Kc//AC2//ライセンスID//コンテンツID//AC1] Km1//CRL_dat } Ks2をデータ端末装置120へ出力する。そして、データ端末装置120のMCU1222は、メモリインタフェース1200を介して暗号化データ { [Kc//AC2//ライセンスID//コンテンツID//AC1] Km1//CRL_dat } Ks2をメモリカード110へ出力する。メモリカード110においては、メモリインタフェース1200を介して、データバスBS4に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてデータバスBS4の受信データを復号しデータバスBS5に出力する(ステップS142)。

【0161】この段階で、データバスBS5には、Km1保持部1421に保持される秘密復号鍵Km1で復号可能な暗号化ライセンス [Kc//AC2//ライセンスID//コンテンツID//AC1] Km1と、CRL_datとが出力される。コントローラ142の指示によって、暗号化ライセンス [Kc//AC2//ライセンスID//コンテンツID//AC1] Km1は、復号処理部1422において、秘密復号鍵Km1によって復号されたライセンス(ライセンス鍵Kc、ライセンスID、コンテンツIDおよび再生回数制限AC1および再生期間AC2)が受理され、ライセンス情報保持部1440に記録される(ステップS146)。

【0162】コントローラ1420は、受理したCRL_datに基づいて、メモリ1415内の禁止クラスリストデータCRLおよびそのバージョンを更新する(ステップS148)。

【0163】ステップS148までの処理がメモリカード110で正常に終了した段階で、携帯電話機100から配信サーバ30にコンテンツデータの配信要求がなされる(ステップS152)。

【0164】配信サーバ30は、コンテンツデータの配信要求を受けて、情報データベース304より、暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infを取得して、これらのデータをデータバスBS1および通信装置350を介して出力する(ステップS154)。

【0165】携帯電話機100は、{Data} Kc/Data-infを受信して、暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infを受信する(ステップS156)。暗号化コンテンツデー

タ {Data} Kcおよび付加情報Data-infは、バスBS3、結合端子1224、およびメモリインタフェース1200を介してメモリカード110のデータバスBS4に伝送される。メモリカード110においては、受信した暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infがそのままメモリ415に記録される(ステップS158)。

【0166】さらに、メモリカード110から配信サーバ30へは、配信受理の通知が送信され(ステップS160)、配信サーバ30で配信受理を受信すると(ステップS162)、課金データベース302への課金データの格納等を伴って、配信終了の処理が実行され(ステップS164)、全体の処理が終了する(ステップS170)。

【0167】このようにして、携帯電話機100のデータ端末装置120に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cmc1とともに暗号化して送信できた公開暗号鍵Kp1およびKmc1が有効であることを確認した上で、それぞれのクラス証明書Cmc1が禁止クラスリスト、すなわち、公開暗号鍵Kp1およびKmc1による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0168】次に、図13および図14を参照してメモリカード110に配信されたコンテンツデータのデータ端末装置120における再生動作について説明する。図13を参照して、再生動作の開始とともに、携帯電話機100のユーザからキー操作部1108を介して再生指示が携帯電話機100にインプットされる(ステップS200)。そうすると、MCU1106は、再生指示をバスBS3および結合端子1224を介してMCU122へ出力する。そして、MCU1222は、データバスBS3を介して認証データ保持部1202から認証データ {Kp1//Crtf1} Kpmaを讀出し、メモリインタフェース1200を介してメモリカード110へ認証データ {Kp1//Crtf1} Kpmaを入力する(ステップS201)。

【0169】そうすると、メモリカード110は、認証データ {Kp1//Crtf1} Kpmaを受理する(ステップS202)。そして、メモリカード110の復号処理部1408は、受理した認証データ {Kp1//Crtf1} Kpmaを、Kpma保持部1414に保持された公開認証鍵Kpmaによって復号し(ステップS203)、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行う。すなわち、認証データ {Kp1//Crtf1} Kpmaが正規の認証データであるか否かを判断する認証処理を行なう(ステップS204)。復号できなかった場

合、コントローラ1420は認証データ不受理の出力をデータバス4および端子1201を介してデータ端末装置120のメモリインタフェース1200へ出力する(ステップS206)。認証データが復号できた場合、コントローラ1420は、取得した証明書Crtf1がメモリ1415から読出した禁止クラスリストデータに含まれるか否かを判断する(ステップS205)。この場合、証明書Crtf1にはIDが付与されており、コントローラ1420は、受理した証明書Crtf1のIDが禁止クラスリストデータの中に存在するか否かを判別する。証明書Crtf1が禁止クラスリストデータに含まれると判断されると、コントローラ1420は認証データ不受理の出力をデータバス4および端子1201を介してリモコン120のメモリインタフェース1200へ出力する(ステップS206)。

【0170】ステップS204において認証データが公開認証鍵Kpmaで復号できなかったとき、およびステップS205において受理した証明書Crtf1が禁止クラスリストデータに含まれているとき、認証データ不受理の出力がなされる。そして、データ端末装置120のMCU1222は、メモリインタフェース1200を介して認証データ不受理の出力を受けると、その旨をバスBS3および結合端子1224を介して携帯電話機100へ出力する(ステップS207)。そして、携帯電話機100のMCU1106は、認証データ不受理のデータをディスプレイ1110に表示する(ステップS207)。

【0171】ステップS205において、証明書Crtf1が禁止クラスリストデータに含まれていないと判断されると、図14を参照して、メモリカード110のセッションキー発生部1418は、再生セッション用のセッションキー-Ks2を発生させる(ステップS208)。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキー-Ks2を、復号処理部1408で復号された公開暗号鍵Kp1によって暗号化した{Ks2}Kp1をデータバスBS4へ出力する(ステップS209)。そうすると、コントローラ1420は、端子1201を介してメモリインタフェース1200へ{Ks2}Kp1を出力し、データ端末装置120のMCU1222は、メモリインタフェース1200を介して{Ks2}Kp1を取得する。そして、Kp1保持部1204は、秘密復号鍵Kp1を復号処理部1205へ出力する。

【0172】復号処理部1205は、Kp1保持部1204から出力された、公開暗号鍵Kp1と対になっている秘密復号鍵Kp1によって{Ks2}Kp1を復号し、セッションキー-Ks2を暗号処理部1208へ出力する(ステップS210)。そうすると、セッションキー発生部1210は、再生セッション用のセッションキー-Ks3を発生させ、セッションキー-Ks3を暗号処理

部1208へ出力する(ステップS211)。暗号処理部1208は、セッションキー発生部1210からのセッションキー-Ks3を復号処理部1206からのセッションキー-Ks2によって暗号化した{Ks3}Ks2を出力し、MCU1222は、データバスBS3およびメモリインタフェース1200を介して{Ks3}Ks2をメモリカード110へ出力する(ステップS212)。

【0173】メモリカード110の復号処理部1412は、端子1201およびデータバスBS4を介して{Ks3}Ks2を入力し、セッションキー発生部1418によって発生されたセッションキー-Ks2によって{Ks3}Ks2を復号して、データ端末装置120で発生されたセッションキー-Ks3を取得する(ステップS213)。

【0174】セッションキー-Ks3の受理に応じて、コントローラ1420は、ライセンス情報保持部1440内の対応するアクセス制限情報AC1を確認する(ステップS214)。

【0175】ステップS214においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC1を確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数に制限があるが、再生可能な場合には、ライセンス情報保持部1440に記録されたアクセス制限情報AC1のデータを更新し再生可能回数を更新した後に次のステップに進む(ステップS215)。一方、アクセス制限情報AC1によって再生回数が制限されている場合においては、ステップS215はスキップされ、再生制御情報AC1は更新されることなく処理が次のステップ(ステップS216)に進行される。

【0176】また、ライセンス情報保持部1440内にリクエスト曲の当該コンテンツIDが存在しない場合においても、再生不可の状態であると判断して、再生動作を終了する。

【0177】ステップS214において、当該再生動作において再生が可能であると判断された場合には、ライセンス情報保持部1440に記録された再生リクエスト曲のライセンス鍵Kcおよび再生回路制御情報AC2がデータバスBS5上に得られる(ステップS216)。

【0178】得られたライセンス鍵Kcと再生回路制御情報AC2は、切換スイッチ1444の接点Pdを介して暗号化処理部1406に送られる。暗号化処理部1406は、切換スイッチ1442の接点Pdを介して復号処理部1412より受けたセッションキー-Ks3によってデータバスBS5から受けたライセンス鍵Kcと再生回路制御情報AC2とを暗号化し、{Kc//AC2}Ks3をデータバスBS3に出力する(ステップS217)。

【0179】データバスBS4に出力された暗号化デー

タは、メモリインタフェース1200を介してデータ端末装置120に送出される。

【0180】データ端末装置120においては、メモリインタフェース1200を介してデータバスBS3に伝達される暗号化データ[Kc/AC2]Ks3を復号処理部1212によって復号処理を行ない、ライセンス鍵Kcおよび再生回路制御情報AC2を受理する(ステップS218)。復号処理部1212は、ライセンス鍵Kc、および再生回路制御情報AC2をデータバスBS3に出力する。

【0181】MCU1222は、データバスBS3を介して、再生回路制御情報AC2を受理して再生の可否の確認を行なう(ステップS219)。

【0182】ステップS219においては、再生回路制御情報AC2によって再生不可と判断される場合には、再生動作は終了される。

【0183】ステップS219において再生可能と判断された場合、MCU1222は、メモリインタフェース1200を介してメモリカード110に暗号化コンテンツデータ(Data)Kcを要求する。そうすると、メモリカード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ(Data)Kcを取得し、データバスBS4および端子1201を介してメモリインタフェース1200へ出力する(ステップS220)。

【0184】データ端末装置120のMCU1222は、メモリインタフェース1200を介して暗号化コンテンツデータ(Data)Kcを取得し、データバスBS3を介して暗号化コンテンツデータ(Data)Kcを復号処理部1214へ与える。また、MCU1222は、復号処理部1212から出力されたバスBS3上のコンテンツ鍵Kcを復号処理部1214へ与える。

【0185】そして、復号処理部1214は、暗号化コンテンツデータ(Data)Kcをコンテンツ鍵Kcによって復号してコンテンツデータDataを取得する(ステップS221)。

【0186】そして、復号されたコンテンツデータDataはMP3デコード1216へ出力され、MP3デコード1216は、コンテンツデータを解凍して再生し、DAC1218はデジタル信号をアナログ信号に変換してジャック1220へ出力する。そして、音楽データはジャック1220を介してヘッドホン130へ出力されて再生される(ステップS222)。これによって再生動作が終了する。

【0187】上述したように、データ端末装置120を含むアダプタ140を用いることにより、暗号化音楽データを配信サーバ30からメモリカード110へダウンロードし、そのダウンロードした暗号化音楽データを復号して再生できる。

【0188】また、アダプタ140を携帯電話機に装着

することによって、データ端末装置120の機能を必要とするユーザはアダプタ140を追加購入すれば、暗号化音楽データを配信サーバ30からメモリカード110へダウンロードし、そのダウンロードした暗号化音楽データを復号して再生できる。

【0189】【実施の形態2】この発明による携帯電話機は、図15に示す携帯電話機100Aであっても良い。携帯電話機100Aは、図3に示す携帯電話機100の本体105を本体105Aに代え、アダプタ140をアダプタ140Aに代えたものであり、その他は携帯電話機100と同じである。本体105Aは、携帯電話機100の本体105にバッテリー150を追加したものであり、その他は本体105と同じである。また、アダプタ140Aは、アダプタ140からバッテリー150を削除したものであり、その他はアダプタ140と同じである。

【0190】バッテリー150は、MCU1108、および音声コーデック1112に駆動電力を供給するとともに、結合端子1118を介してアダプタ140Aのデータ端末装置120にも駆動電力を供給する。

【0191】携帯電話機100Aを用いても、実施の形態1において説明したのと同じ方法によって配信サーバ30からメモリカード110へ暗号化音楽データをダウンロードできるとともに、メモリカード110から暗号化音楽データを読み出し、復号および再生を行なうことができる。

【0192】携帯電話機100Aは、バッテリー150が本体105Aの駆動電力と、データ端末装置120の駆動電力とを賄うことができる容量を持っている場合、アダプタ140Aのみを購入すれば、暗号化音楽データのダウンロードおよび復号・再生を行なうことができる。したがって、携帯電話機100Aのユーザはアダプタ140Aだけを購入し、自己の携帯電話機にアダプタ140Aを装着することによって携帯電話機100Aを用いて、暗号化音楽データをダウンロードし、その暗号化音楽データを再生して聴くことができる。本実施の形態2においてはバッテリー150を本体105Cに備えるように説明したが、バッテリー150は本体105Cにコネクタ等で接続されていて、本体105Cから着脱可能な構造としてもよい。

【0193】【実施の形態3】この発明による携帯電話機は、図16に示す携帯電話機100Bであっても良い。携帯電話機100Bは、図3に示す携帯電話機100の本体105を本体105Bに代え、アダプタ140をアダプタ140Bに代えたものであり、その他は携帯電話機100と同じである。本体105Bは、携帯電話機100の本体105に混合回路1124を追加し、ジャック1114をジャック1122に代えたものであり、その他は本体105と同じである。また、アダプタ140Bは、携帯電話機100のアダプタ140からジ

ジャック 1220 を削除したものであり、その他はアダプタ 140 と同じである。

【0194】混合回路 1124 は、音声コーデック 112 によって復調およびデジタル信号からアナログ信号への変換が行われた音声データをジャック 1122 へ出力する。また、混合回路 1124 は、アダプタ 140 B のデータ端末装置 120 によって復号および再生が行われた音楽データを結合端子 1118 を介して受取り、その受取った音楽データをジャック 1122 へ出力する。

【0195】ジャック 1122 は、混合回路 1124 から音声データまたは音楽データをヘッドホン 130 へ出力する。また、ジャック 1122 は、携帯電話機 100 B のユーザが話した音声データをマイク（図示せず）を介して受取り、音声コーデック 1112 へ出力する。なお、ジャック 1122 は、マイクからの音声データを入力し、2 チャンネルの音楽データまたは音声データをヘッドホン 130 へ出力するため、4 芯のジャックとなっている。また、1 つのジャックを介して音声データを入力し、音楽データを出力するので、携帯電話機による通常の通話を行ないながら、音楽を聴くことができる。その他は、実施の形態 1 の説明と同じである。

【0196】携帯電話機 100 B を用いても、実施の形態 1 において説明したのと同じ方法によって配信サーバ 30 からメモ리카ード 110 へ暗号化音楽データをダウンロードできるとともに、メモ리카ード 110 から暗号化音楽データを読み出し、復号および再生を行なうことができる。

【0197】【実施の形態 4】この発明による携帯電話機は、図 17 に示す携帯電話機 100 C であっても良い。携帯電話機 100 C は、図 18 に示す携帯電話機 100 B の本体 105 B を本体 105 C に代え、アダプタ 140 B をアダプタ 140 C に代えたものであり、その他は携帯電話機 100 B と同じである。本体 105 C は、携帯電話機 100 B の本体 105 B にバッテリー 150 を追加したものであり、その他は本体 105 B と同じである。また、アダプタ 140 C は、アダプタ 140 B からバッテリー 150 を削除したものであり、その他はアダプタ 140 B と同じである。

【0198】バッテリー 150 は、MCU 1106、音声コーデック 1112、および混合回路 1124 に駆動電力を供給するとともに、結合端子 1118 を介してアダプタ 140 C のデータ端末装置 120 にも駆動電力を供給する。

【0199】携帯電話機 100 C を用いても、実施の形態 1 において説明したのと同じ方法によって配信サーバ 30 からメモ리카ード 110 へ暗号化音楽データをダウンロードできるとともに、メモ리카ード 110 から暗号化音楽データを読み出し、復号および再生を行なうことができる。

【0200】携帯電話機 100 C は、バッテリー 150 が本体 105 C の駆動電力と、データ端末装置 120 の駆動電力とを賄うことができる容量を持っている場合、アダプタ 140 C のみを購入すれば、暗号化音楽データのダウンロードおよび復号・再生を行なうことができる。そして、携帯電話機 100 C のユーザは 1 つのジャック 1122 を介して通常の電話機能による音声データと、音楽データをステレオおよびモノラルで聴くことができる。その他は、実施の形態 1、3 と同じである。

10 【0201】本実施の形態においてはバッテリー 150 を本体 105 C に備えるように説明したが、バッテリー 150 は本体 105 C にコネクタ等で接続されていて、本体 105 C から着脱可能な構造としてもよい。

【0202】また、実施の形態 1~4 において、アダプタ 140 には暗号化コンテンツデータまたはラジエンスの配信を受け、暗号化コンテンツデータを再生するデータ端末装置 120 を備えるように説明したが、必ずしも両機能を備える必要はなく、配信を受ける機能と暗号化コンテンツデータを再生する機能のいずれか一つのみを行なうデータ端末装置を備えるものであってもよい。

20 【0203】さらに、実施の形態 1~4 において、MP3 方式によって符号化された音楽データを扱うように説明したが、特に、MP3 に限定するものではなく、音楽が生成可能なデジタルデータであればいかなる符号化方式によって符号化された音楽データであってもよい。

【0204】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

30 【図面の簡単な説明】

【図 1】データ配信システムを概念的に説明する概略図である。

【図 2】本発明による携帯電話機の裏面の平面図である。

【図 3】実施の形態 1 による携帯電話機の概略ブロック図である。

【図 4】図 1 に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

40 【図 5】図 1 に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図 6】図 1 に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図 7】ライセンスサーバの構成を示す概略ブロック図である。

【図 8】実施の形態 1 における携帯電話機の構成を示すブロック図である。

50 【図 9】図 3 に示す携帯電話機に含まれるデータ端末装置の構成を示すブロック図である。

【図10】 実施の形態1におけるメモリカードの構成を示すブロック図である。

【図11】 図1に示すデータ配信システムにおける配信動作を説明するための第1のフローチャートである。

【図12】 図1に示すデータ配信システムにおける配信動作を説明するための第2のフローチャートである。

【図13】 実施の形態1における携帯電話機における再生動作を説明するための第1のフローチャートである。

【図14】 実施の形態1における携帯電話機における再生動作を説明するための第2のフローチャートである。

【図15】 実施の形態2における携帯電話機の構成を示すブロック図である。

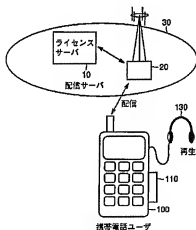
【図16】 実施の形態3における携帯電話機の構成を示すブロック図である。

【図17】 実施の形態4における携帯電話機の構成を示すブロック図である。

【符号の説明】

10 ライセンスサーバ、20 配信サーバ、30 配信サーバ、100、100A、100B、100C 携帯電話機、105、105A、105B、105C 本体、110 メモリカード、120 データ端末装置、130 ヘッドホン、140、140A、1540*

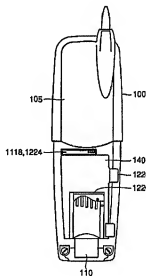
【図1】



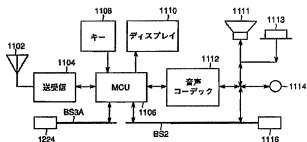
*B、140C アダプタ、150 バッテリ、302 課金データベース、304 情報データベース、306

CRLデータベース、310 データ処理部、312、320、1205、1212、1404、1408、1412、1422 復号処理部、315 配信制御部、316、1210、1418 セッションキー発生部、318、326、328、1208、1406、1410 暗号処理部、350 通信装置、1102 アンテナ、1104 送受信部、1106、1222 MCU、1108 キー操作部、1110 ディスプレイ、1111 スピーカ、1112 音声コーデック、1113 マイク、1218 DAC、1114、1220 ジャック、1201 端子、1116 パッド、1118、1224 結合端子、1124 混合回路、1200 メモリインタフェース、1202、1400 認証データ保持部、1204 Kp1保持部、1206 公開復号部、1214 DES、1216 MP3デコード、1226 着脱部、1230 共通鍵暗号・復号部、1402 Kmcl保持部、1414 Kpma保持部、1415 メモリ、1416 Kpml保持部、1420 コントローラ、1421 Km1保持部、1440 ライセンス情報保持部、1442、1444、1446 切換スイッチ。

【図2】



【图8】



【圖4】

名称	属性	保持/発生期間	検出・特徴
Data1	コンテンツデータ		音楽データ
Ko	ライセンス鍵		暗号化コンテンツデータの復号鍵
(Date)Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化データとされたコンテンツデータ この形式で配信サーバに配布
Data-Inf	付随情報		例：コンテンツデータに関する著作権あるいは サーバアクセス履歴等の文字情報
ID	コンテンツに関する情報	配信サーバ	コンテンツデータDataを識別するコード
ライセンスID	コンテンツに関する情報		ライセンスの発行を特定するための管理コード (コンテンツIDと組み合わせて利用することも可)
AC	ライセンス購入条件		利用者を何ぞ指定(例：ライセンス数、販売先決定等)
AA1	アクセス制限情報		メモリのアクセスに対する制限(例：書き込み回数)
AA2	再生制御情報		コンテンツの再生回数(複製や盗聴)における制御情報 (例：再生回数)

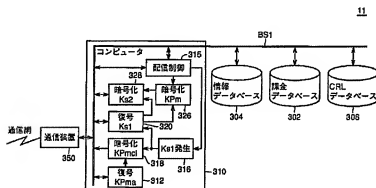
【圖6】

名称	属性	保持・発生箇所	機能・特徴
Ka1	共通種	配信サーバ	配信セッション毎に発生
Ka2		メモリカード	配信・再生セッション毎に発生
Ka3		データ廃棄装置	再生セッション毎に発生
Km	簡易符号種	メモリカード	メモリカードごとに固有の発号種
KPm	公開符号種 (非対称鍵)	メモリカード	KPmで発号ごとに固有の発号種と復号可能
KPma	公開対称鍵	配信サーバ	配信システム全体で共通。

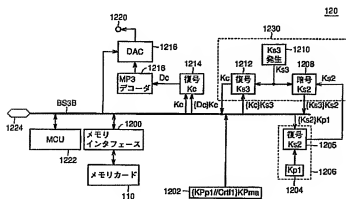
【圖5】

名称	属性	保持/発生箇所	補綴・特徴
CRL	禁止クラスリスト	配布サーバ メモリカード	禁止クラスリストの対象クラスデータ
CRL_dai	禁止クラスリスト 関連情報	メモリカード	禁止クラスリストのバージョン更新のための情報 (連番データ形式)
CRL_ver		メモリカード	禁止クラスリストのバージョン情報
KPpn	公開暗号鍵 (非対称鍵)	データ端末装置	Kpnicにて使用可能。 (KpPn/KpPmaの形式で出荷時に記録 ※データ端末装置の機能ごとに異なる)
KPmci	公開暗号鍵 (非対称鍵)	メモリカード	Kmicnicにて使用可能。 (KpMci/KpMciPmaの形式で出荷時に記録 ※データ端末装置の機能ごとに異なる)
Kpni	秘密暗号鍵	データ端末装置	コピー制御機能 (データ端末装置) 固有の復号鍵 ※データ端末装置の機能ごとに異なる
Kmci	秘密暗号鍵	メモリカード	メモリカード固有の復号鍵 ※メモリカードの機能ごとに異なる
Crlin		データ端末装置	コピー制御機能 (データ端末装置) 記録機能をする。 (KpPn/KpPmaの形式で出荷時に記録 ※データ端末装置のクラスごとに異なる)
Cmci	クラス証明書	メモリカード	メモリカードのクラス証明書。記録機能をする。 (KpMci/KpMciPmaの形式で出荷時に記録 ※メモリカードのクラスごとに異なる)

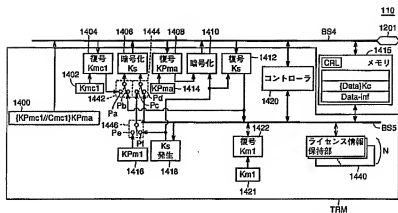
【圖7】



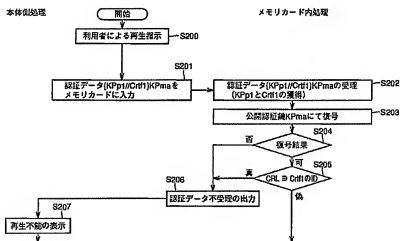
【圖9】



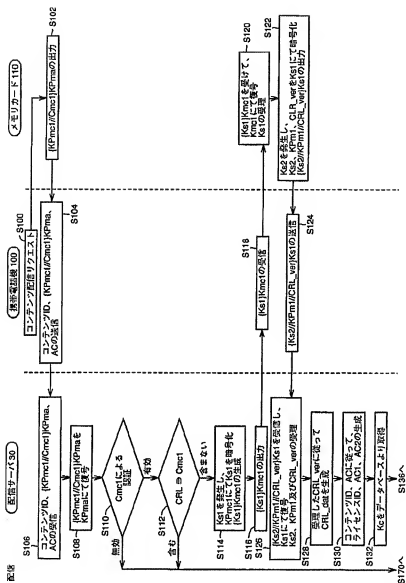
【圖 10】



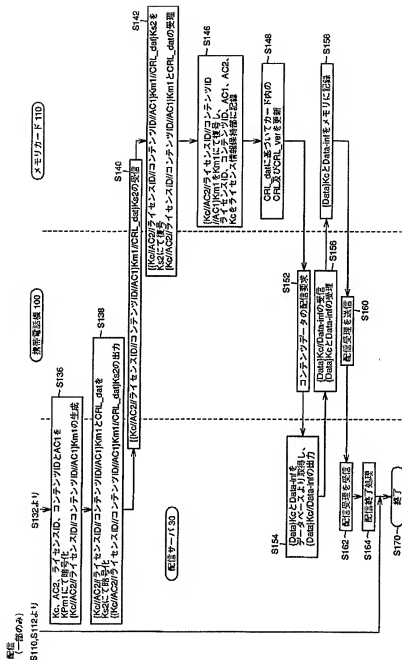
【圖13】



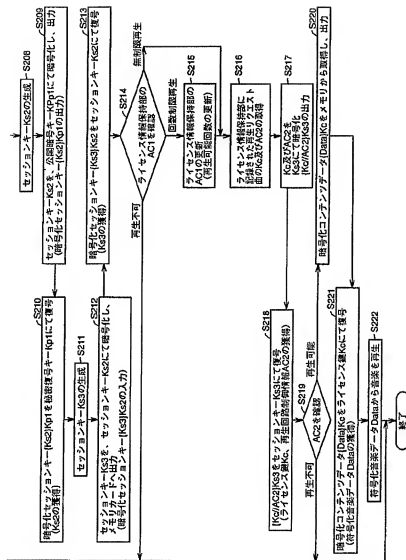
【図 11】



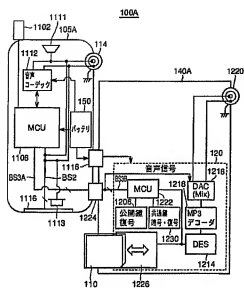
[図 12]



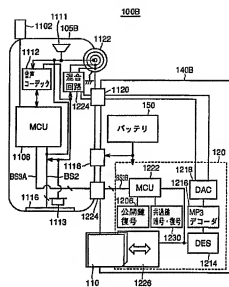
【図14】



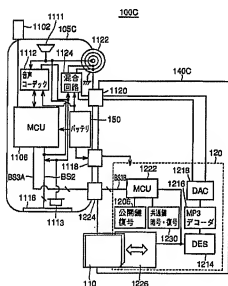
【図15】



【図16】



【図17】



フロントページの続き

(51)Int. Cl.⁷

H04L 9/32

H04M 1/00

1/02

1/725

11/00

識別記号

302

FI

H04M 11/00

G10L 9/00

H04B 7/26

H04L 9/00

キーワード(参考)

302

N

M

601B

601E

F ターム(参考) SJ104 AA07 AA16 EA06 EA19 EA22
KA02 KA05 NA03 NA35 NA37
NA41 NA42 NA43 PA02
SK023 AA07 MA21 PP01 PP11
SK027 AA11 FF01 FF25 HH26
SK067 AA32 BB04 DD54 DD57 EE02
EE10 EE16 FF26 FF40 HH07
HH23 HH36 KK05 KK15
SK101 KK18 LL12 NN01 NN15 NN21